UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,607	06/01/2001	Christophe Clavier	032326-132	2078

21839 7590 08/05/2008

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

NOTIFICATION DATE	DELIVERY MODE
08/05/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	09/807,607	CLAVIER ET AL.	
	Examiner	Art Unit	
	KAVEH ABRISHAMKAR	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 13-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 13-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This communication is in response to the amendment filed on March 17, 2008. Claims 1-10, and 13-16 were pending consideration.

2. The Terminal disclaimer filed on March 17, 2008 obviates the double patenting rejection.

Response to Arguments

Applicant's arguments with respect to claims 1-16 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-9, and 13, and 15-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Akkar et al. (U.S. Patent Pub. No. US 2001/0012360 A1).

Regarding claim 1, Akkar discloses:

A countermeasure method against attacks by differential analysis of current consumption in an electronic component using a cryptographic algorithm having a

secret key, comprising the following steps

executing a first set of instructions in the algorithm that are critical to said attacks with a first manipulating means to deliver output data on the basis of input data (paragraph 0026: *using operation O, corresponding to conventional DES*); and

executing another set of said critical instructions with other manipulating means that are derived from said first manipulating means by complementation of at least one of said input data and said output data, so that the output data and data derived from said output data are unpredictable (paragraph 0026-0027: *wherein another operation is performed (O's complement) in a random manner*).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Akkar discloses:

A countermeasure method according to claim 1, wherein said first and said other manipulating means are selected on the basis of one-half probability statistical relationship (paragraph 0027: *wherein the operations are selected in a random manner, and since there are 2 operations, there is a ½ chance of either being selected*).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Akkar discloses:

A countermeasure method according to claim 2, wherein said algorithm comprises sixteen rounds, and wherein said method comprises executing a first sequence and a second sequence, each of which is made up of at least the first three

rounds, such that the order in which the sequences are executed is a function of the one-half probability statistical relationship, with the first sequence using the first manipulating means in each round, and the second sequence using the other manipulating means in at least the first round (paragraph 0027: *wherein the operations are selected in a random manner, and since there are 2 operations, there is a ½ chance of either being selected*).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Akkar discloses:

A countermeasure method according to claim 3, wherein each of the first and second sequences is made up of the first three rounds (paragraph 26: *wherein the encryption is performed by DES, and can include any number of rounds*).

Claim 5 is rejected as applied above in rejecting claim 3. Furthermore, Akkar discloses:

A countermeasure method according to claim 3, wherein said other manipulating means consist of second means such that, for the same input data, the complement of the output data of the first manipulating means is produced as output data (paragraph 0026-0027: *wherein another operation is performed (O's complement) in a random manner*).

Claim 6 is rejected as applied above in rejecting claim 2. Furthermore, Akkar discloses:

A countermeasure method according to claim 2, wherein said algorithm comprises sixteen rounds, and wherein said method comprises executing a first

sequence and a second sequence, each of which is made up of at least the first three rounds, such that the order in which the sequences are executed is a function of the one-half probability statistical relationship, with the first sequence using the first manipulating means in each round, and the second sequence using the other manipulating means (paragraph 0026-0027: wherein the first operation (O) is DES (16 rounds), and *wherein another operation is performed (O's complement) in a random manner*).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Akkar discloses:

A countermeasure method according to claim 6, wherein each of the first and second sequences are made up of the last three rounds, and wherein the other manipulating means used in the second sequence comprise second manipulating means and a third manipulating means (paragraph 26: *wherein the encryption is performed by DES, and can include any number of rounds*).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Akkar discloses:

A countermeasure method according to claim 7, wherein said second manipulating means are such that, for the same input data, the complement of the output data of the first manipulating means is produced as output data, and wherein said second manipulating means are used in the second sequence for the fourteenth round (paragraph 0026-0027: *wherein the encryption is performed by DES, and can*

include any number of rounds and wherein another operation is performed (O's complement) in a random manner).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Akkar discloses:

A countermeasure method according to claim 8, wherein said third manipulating means are such that, for the complement of the input data, the complement of the output data of the first manipulating means is produced as output data, and wherein said third manipulating means are used in the second sequence for the fifteenth round and the sixteenth round (paragraph 26: *wherein the encryption is performed by DES, and can include any number of rounds*).

Regarding claim 13, Akkar discloses:

An electronic component which provides countermeasures against attacks on a secret key cryptographic algorithm, comprising:

a program memory having stored thereon a plurality of different manipulating means for producing output data in response to input data (paragraph 0026-0027: *wherein the first operation (O) is DES, and wherein another operation is performed (O's complement) in a random manner*).

Claim 15 is rejected as applied above in rejecting claim 13. Furthermore, Akkar discloses:

The electronic component of claim 13 wherein said different manipulating means respectively produce sets of output data that are complementary to one another (paragraph 0026-0027: *wherein the first operation (O) is DES, and wherein another operation is performed (O's complement) in a random manner*).

Claim 16 is rejected as applied above in rejecting claim 13. Furthermore, Akkar discloses:

The electronic component of claim 13, wherein said component is a smart card (paragraph 0026: *a smart card*).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 10 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Akkar et al. (U.S. Patent Pub. No. US 2001/0012360 A1) in view of Kocher (U.S. Patent 6,278,783).

Claim 10 is rejected as applied above in rejecting claim 1. Akkar does not explicitly teach wherein said manipulating means are a table of constants. Kocher discloses that manipulating means are constants tables (column 7, lines 15-65). Kocher teaches the

uses of tables to manipulate data. These tables are filled with parameters (constants) that are updated so that attackers cannot obtain the contents of the table by an analysis of measurements. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the tables of constants to minimize information leakage when using an electronic component such as a smart card (Kocher: Abstract).

Claim 14 is rejected as applied above in rejecting claim 13. Akkar does not explicitly teach wherein said manipulating means are a table of constants. Kocher discloses that manipulating means are constants tables (column 7, lines 15-65). Kocher teaches the uses of tables to manipulate data. These tables are filled with parameters (constants) that are updated so that attackers cannot obtain the contents of the table by an analysis of measurements. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the tables of constants to minimize information leakage when using an electronic component such as a smart card (Kocher: Abstract).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Examiner, Art Unit 2131

/K. A./
07/31/2008
Examiner, Art Unit 2131